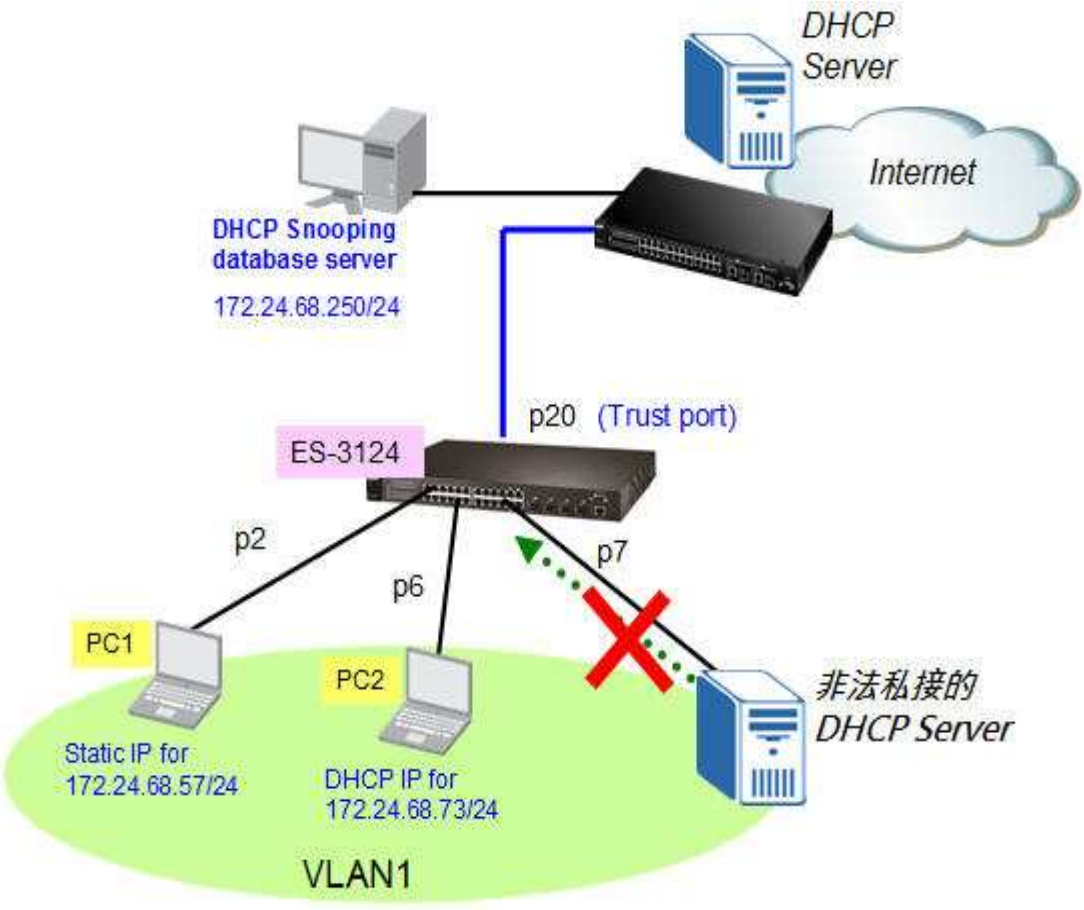
Switch 設備如何設定應用 IP Source Guard

需求說明：

對於企業或校園等機關團體，資料保密性相當重要，為了不讓使用者私帶個人電腦接上內部網路進行資料下載、上網，或是私接寬頻路由器(IP 分享器) 以致影響正常網路運作。一般防制作法除了搭配認證設備對欲進行網路使用的使用者進行複雜的身分驗證外，另外也可簡易透過 Switch 設備中關於 IP Source Guard (IP/MAC Binding) 此功能來達到，此文件範例將教導各位如何進行相關設定及驗證測試。

範例架構拓撲圖:



附註 1： 設定此功能時建議請使用交換器 Management(MGMT) Port 來進行設定，以避免啟用 ARP Inspection 功能後即無法控管該交換器。而欲使用 MGMT Port 對交換器進行設定，請將設定交換器用的電腦 IP 設定成 192.168.0.X/24，2 < X < 254

附註 2： IP Source Guard 功能由兩部分所組成，其一為 DHCP Snooping 或 Static Binding (此功能作用為建立一合法網路設備清單，在此清單上的網路設備才可正常的使用網路，否則一律視為非法設備無法使用)，其二為 ARP Inspection(此功能作用為依照前者的合法清單內容，放行或拒絕由交換器所偵測到的 ARP 封包)。

附註 3：關於 DHCP snooping 此功能設定，觀念步驟如下:

Step1. 啟動 DHCP snooping 此功能

Step 2. 在 Switch 內每個 VLAN 設定中, 啟動 DHCP snooping 此功能

Step 3. 規劃設定 trusted 以及 untrusted ports

Step 4. 依需求決定是否新增設定 static bindings.

附註 4：關於 ARP inspection 此功能設定，觀念步驟如下:

Step 1 首先設定完成 DHCP snooping 相關功能

Step 2 在 Switch 內每個 VLAN 設定中, 啟動 ARP inspection 此功能

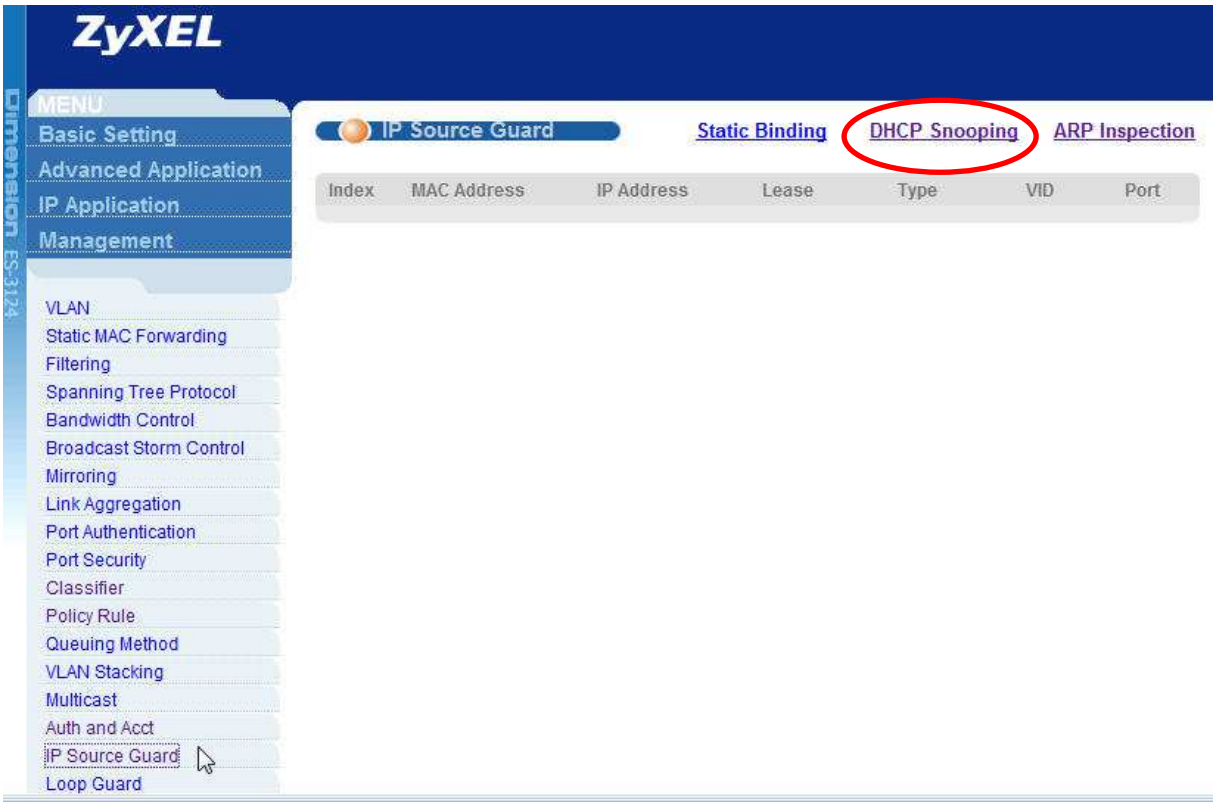
Step 3 規劃設定 trusted 以及 untrusted ports.

交換器設定說明:

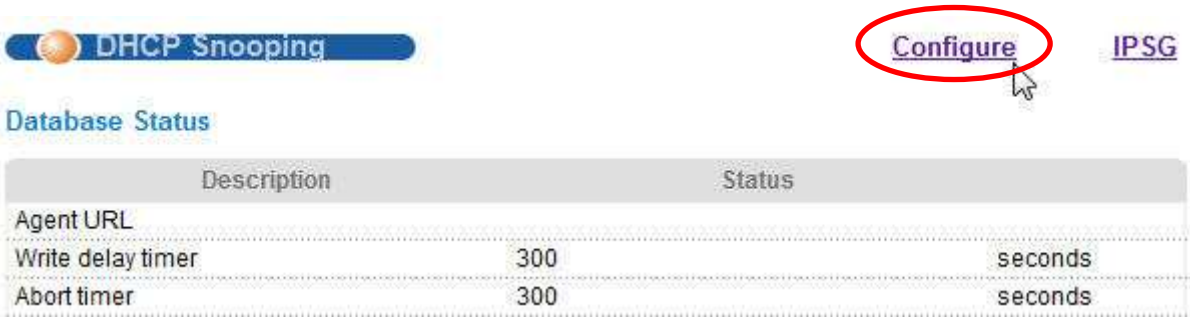
第一部分：DHCP Snooping 或 Static Binding 設定

(1)For dynamic IP(動態 IP 位址綁定)設定如下步驟：

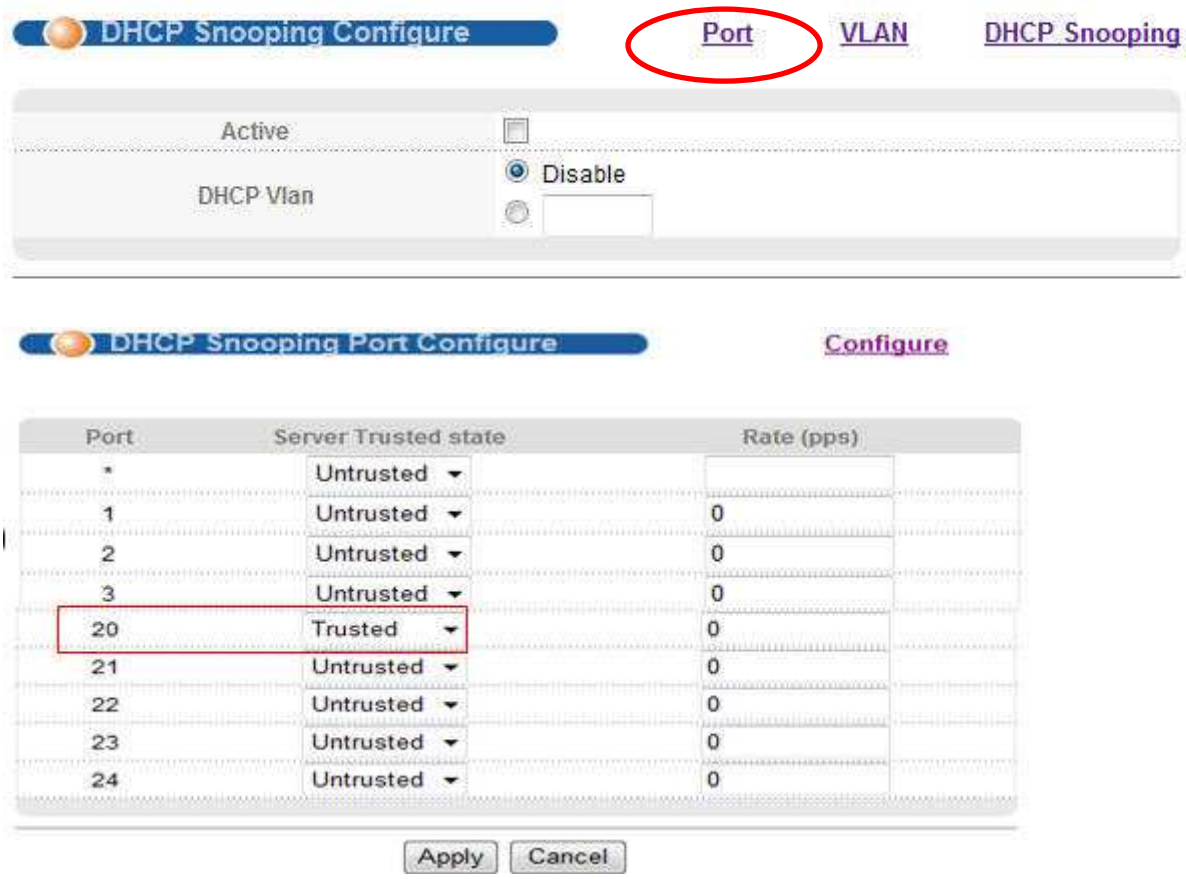
步驟 1：在 **Advanced Application** > **IP Source Guard** 此頁面點選，點選 DHCP Snooping



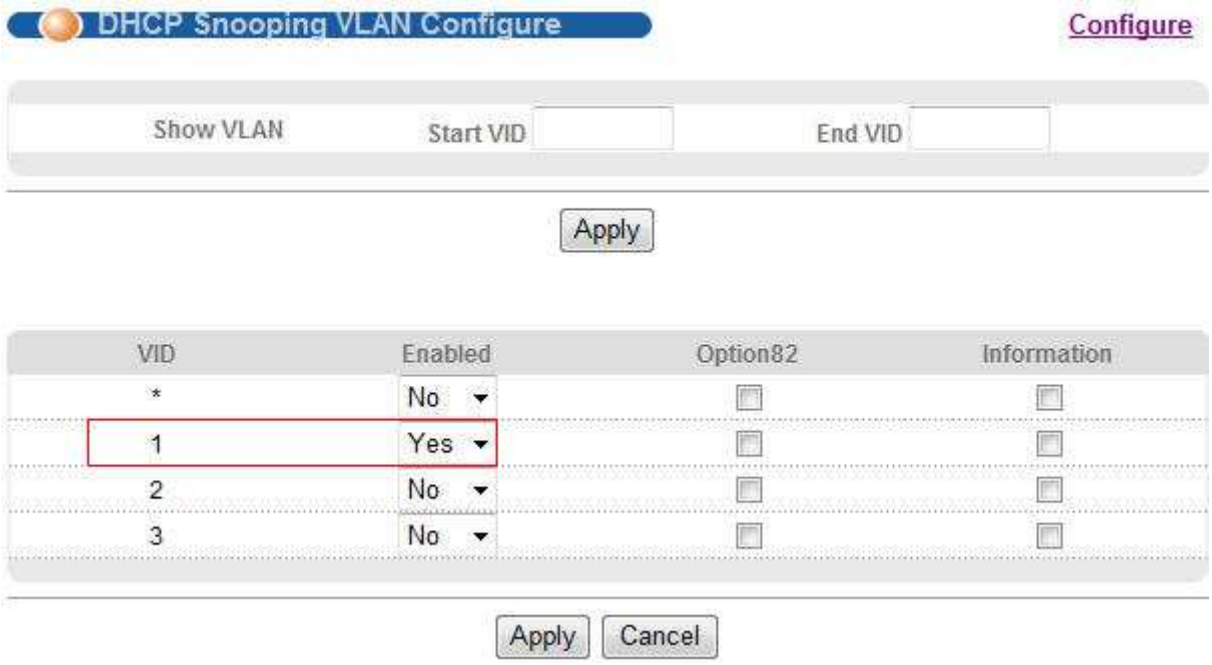
步驟 2：點選 Configure



步驟 3：點選 Port，設定 Trust port(這邊範例為由 port20 介接上端 DHCP Sever)

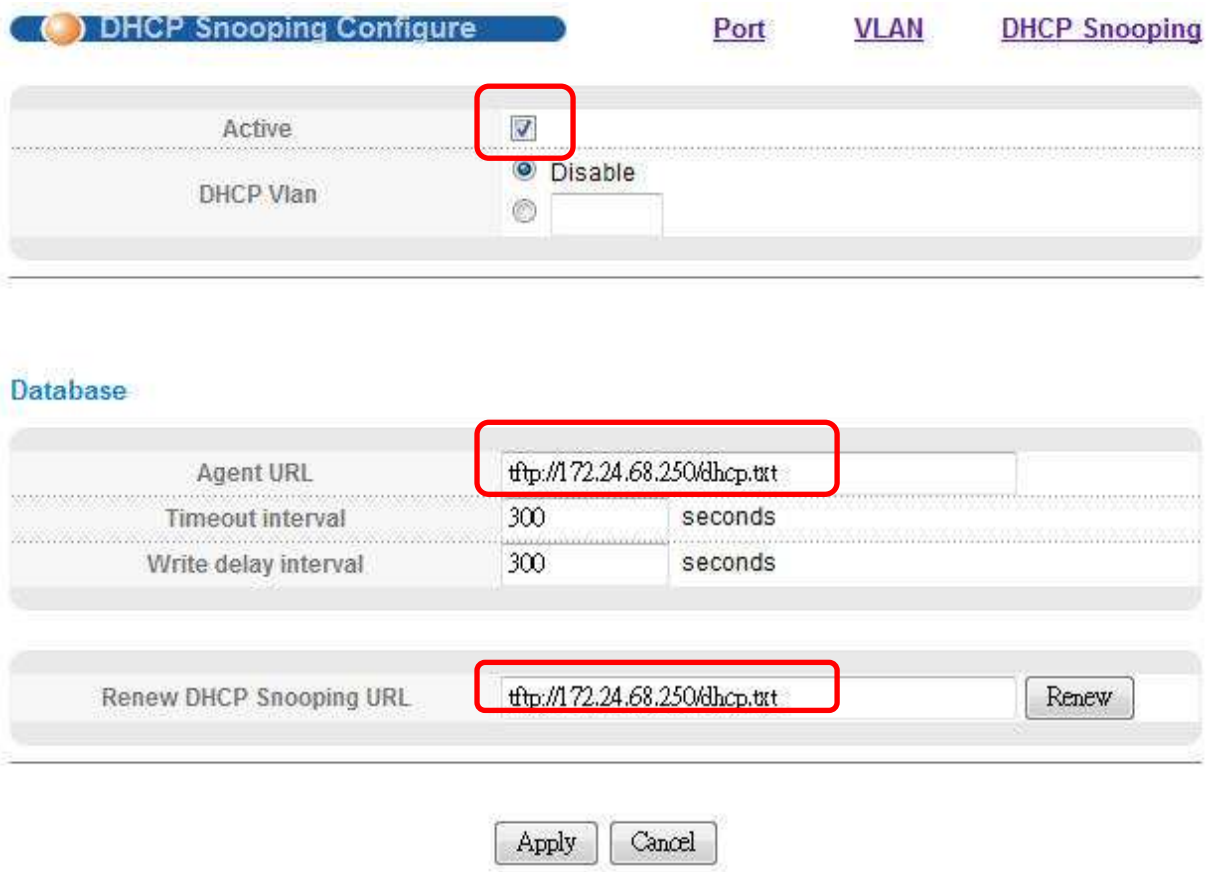


步驟 4：切換回主頁面，點選 VLAN (這邊範例為將 VLAN1 設為 Yes 啟動)



步驟 5：切換回主頁面，將此功能打勾 Active，另外關於 Database 設定欄位建議也需要設定，

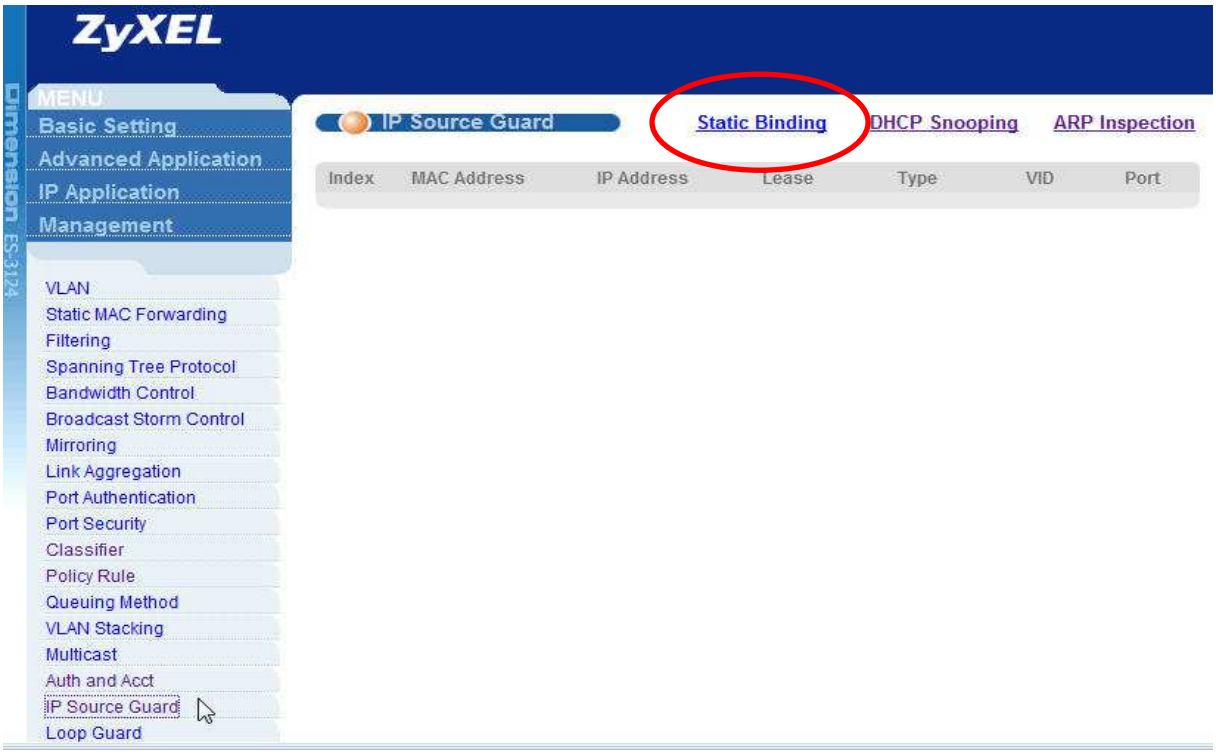
請於網路環境中架設一台 DHCP Snooping database server(TFTP Server) 來儲存動態的 dynamic **binding** table，否則若交換器有手動重開機狀況發生，則動態 dynamic **binding** table 將會被清除，請注意!交換器只會保留靜態 **static binding** table !



步驟 6：此時 PC2 電腦網路線重新插拔後，待檢查 Timer 時間到後，即會在選單看到如下所示的 dynamic **binding** table，此代表完成正確設定。(若電腦網卡由 DHCP 方式取得 IP 位址，當成功設定 DHCP Snooping 功能後，則 table 中的 Lease 欄位與 Type 欄位會顯示為 0d9h59m55s 與 dhcp-snooping 此格式。

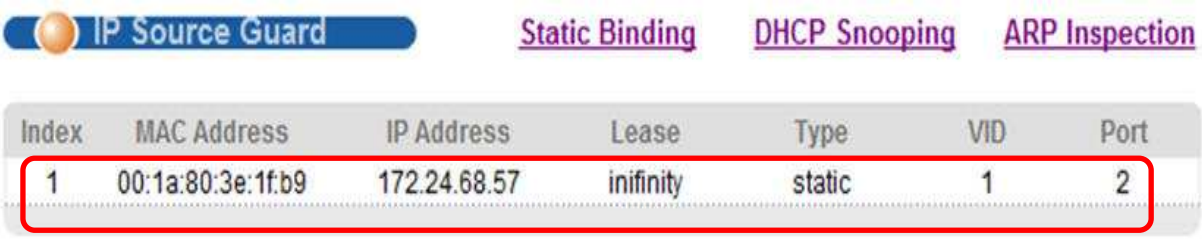
(2)For **Static Binding**(靜態 IP 位址綁定)設定如下步驟：

步驟 1: 在 **Advanced Application** > **IP Source Guard** 此頁面點選，點選 **Static Binding**，建立一筆靜態合法清單內容。



步驟 2：在此輸入您准許使用之網路設備 MAC 位址、IP 位址、VLAN 與 Port，最後點選 **Add** 進行新增。

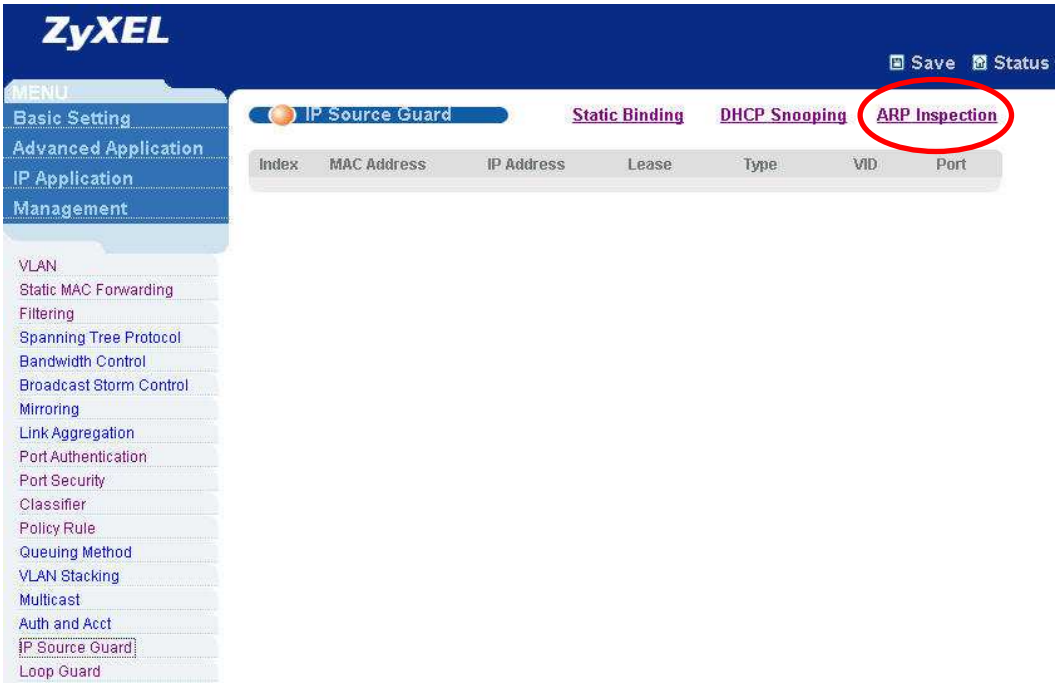
步驟 3：點選該頁面右上角之 **IPSG** 回到 IP Source Guard 功能設定頁面，在此即可立刻檢視您剛設定之 PC1 電腦資料。(若是電腦網卡為 Static IP 位址，故在 Lease 欄位顯示為 inifinity，Type 欄位顯示為 static 此格式。)



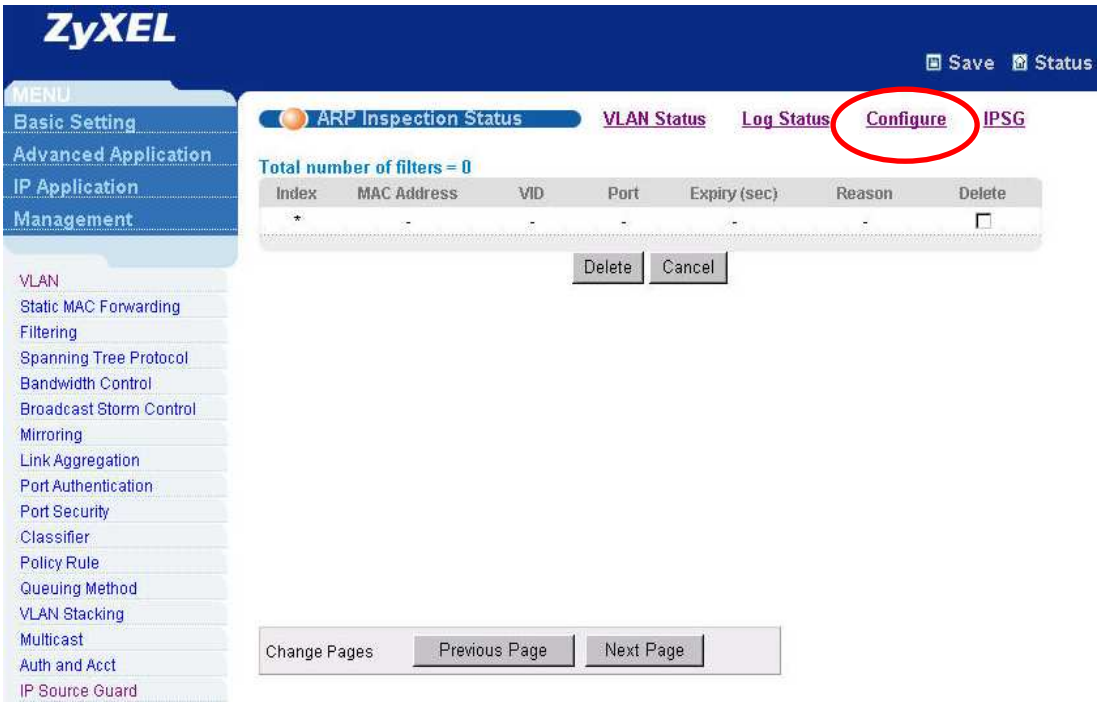
依照以下設定範例即完成設備合法清單之設定，接下來需設定 ARP Inspection 功能來過濾合法與非法的 ARP 封包。

第二部分：設定 ARP Inspection

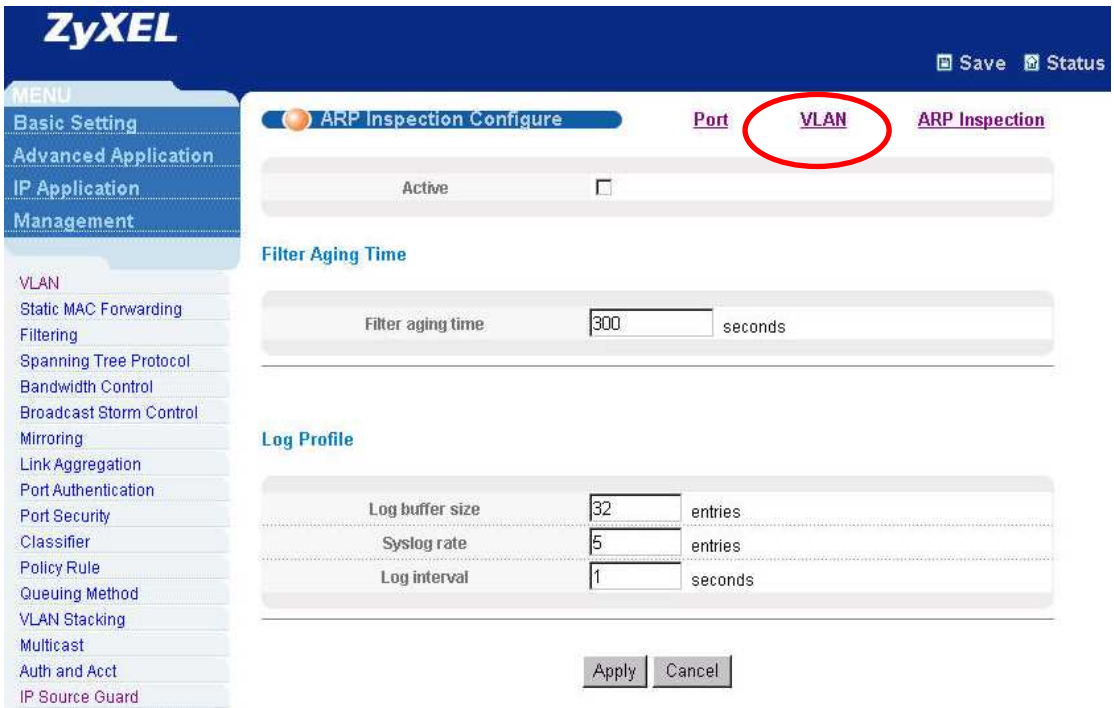
步驟 1：點選 **ARP Inspection 來達到**過濾網路上非法之 ARP 封包。



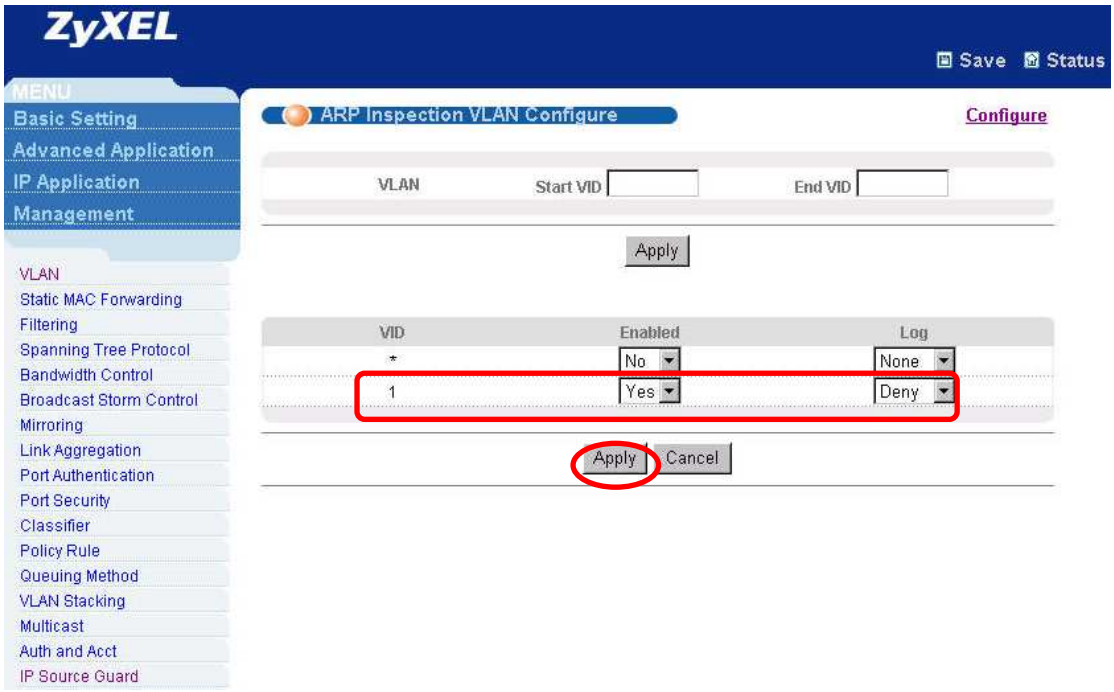
步驟 2：點選 **Configure** 組態相關設定。



步驟 3：點選 **VLAN** 好在個別 VLAN 分別啟用 ARP Inspection。



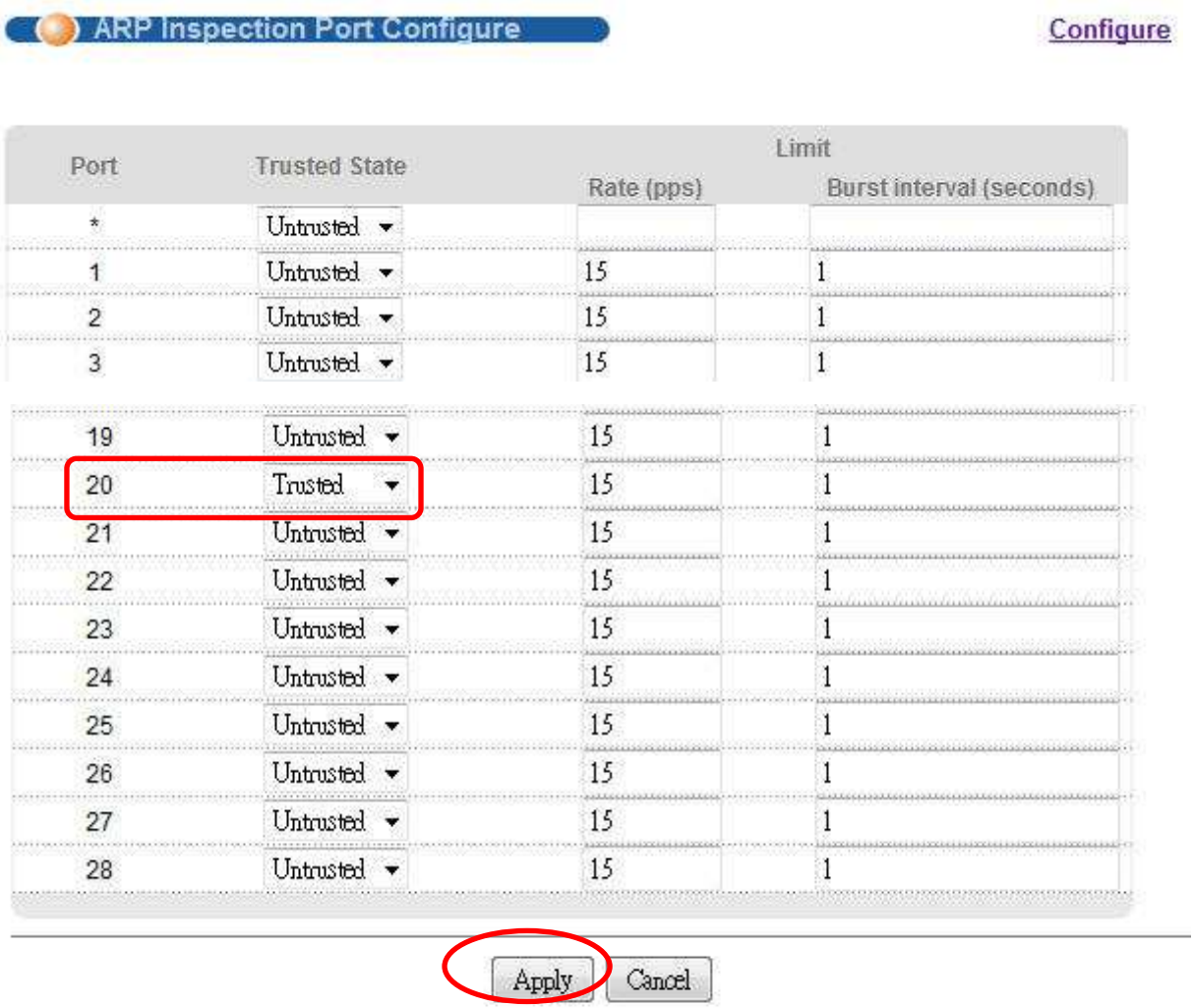
步驟 4：在此以 VLAN1 為設定範例。分別在 **Start VID** 與 **End VID** 輸入 VLAN 範圍，例如前後欄位各輸入「1」，然後點選 **Apply** 進行確認。如圖所示，請在 VID 1 Enabled 欄位點選「Yes」，最後點選 **Apply** 進行設定值套用即可。



步驟 5：設定完成後，點選此頁面之右上角之 **Configure** 回到 ARP Inspection 相關設定頁面。

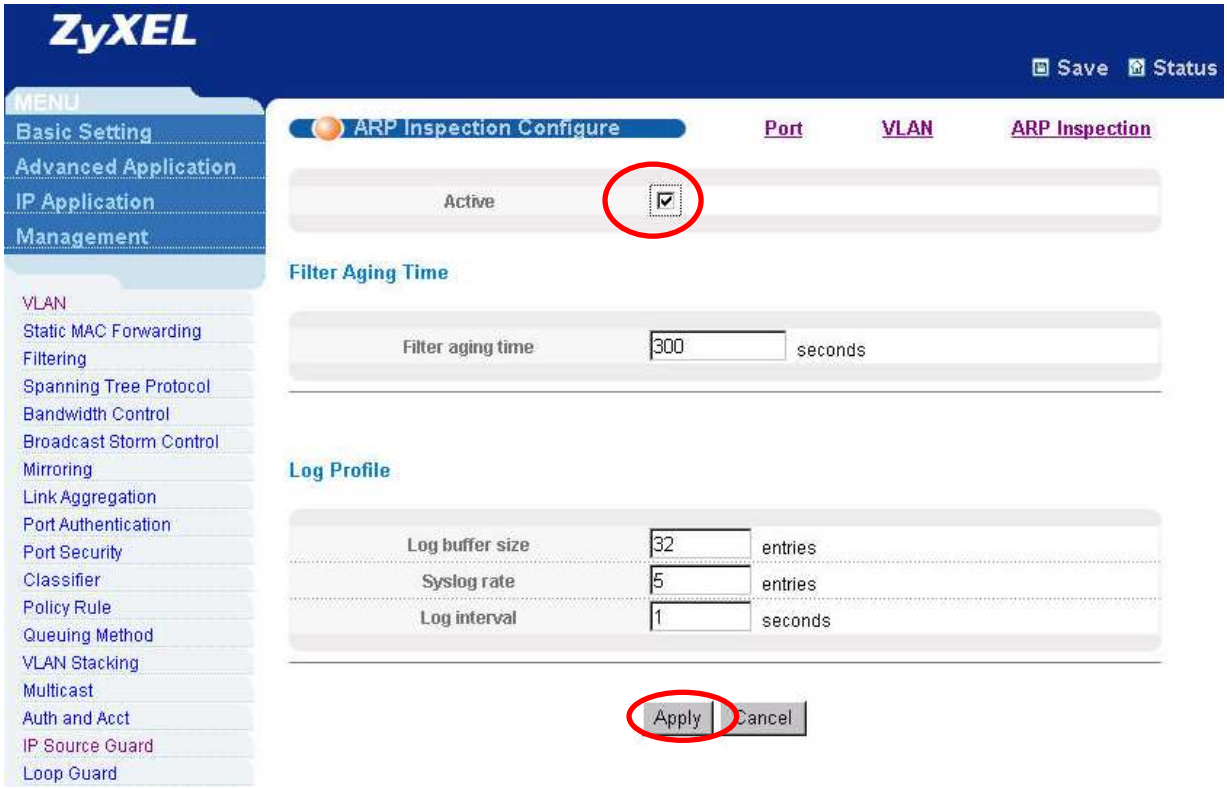
步驟 6：點選此頁面之 **Port** 進行 port 狀態設定。對於 ARP Inspection 功能，Port 分成兩種狀態，一為信任**(Trusted)Port**、另一為不信任**(Untrusted)Port**。ARP 封包「永遠」不會被 ARP Inspection 信任的 Port 所丟棄，但不信任的 Port 之 ARP 封包會被丟棄，前提是該 ARP

封包的來源 MAC、VLAN 資訊不在合法清單內或在規定時間內所接收到的 ARP 封包頻率超過合法設定值。依架構拓撲圖說明，在 Port20 設定為 **Trusted Port**，最後點選 Apply 進行套用。



步驟 7：設定完成後，點選此頁面之右上角之 **Configure** 回到 ARP Inspection 相關設定頁面。

步驟 8：最後勾選 **Active**，啟用 ARP Inspection 功能，並點選 Apply 進行套用。



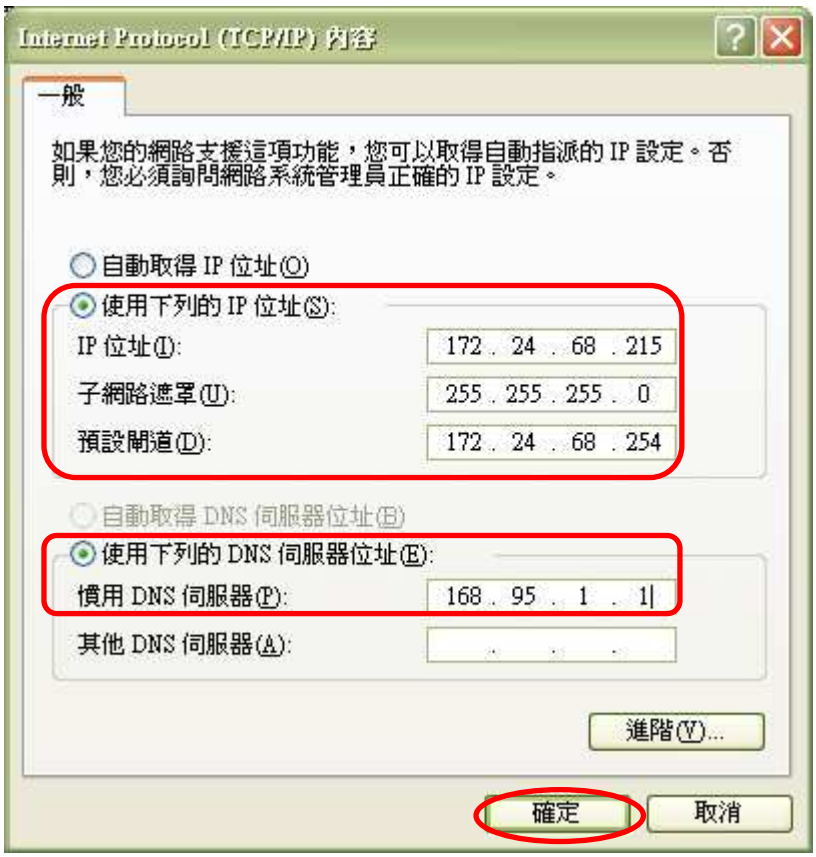
第三部分：測試驗證

先由一部合法網路設備(PC2)成功取得 DHCP Server 配發之 IP，然後測試可否正常執行任何網路運作，接著由該手動變更網卡 IP 位址，其 IP 位址為原本 DHCP pool 範圍內，測試 IP Source Guard 功能是否成功偵測與拒絕該變更過後的非法 IP 位址。

步驟 1：將合法網路設備(PC2)串接至 ES-3124 的 Port 6，並成功由 DHCP Server 取得 IP，然後進行網路服務測試，例如：Ping HiNet DNS Server，此時會發現可成功藉由 ARP Request 封包得知 Gateway MAC 位址。

步驟 2：停用 NB 網路卡介面，目的為變更 IP 配置為手動設定。

步驟 3：將 IP 位址由 DHCP 配置變更為手動配置，配置資訊如圖所示，設定完畢後，請點選**確定**進行設定值套用。

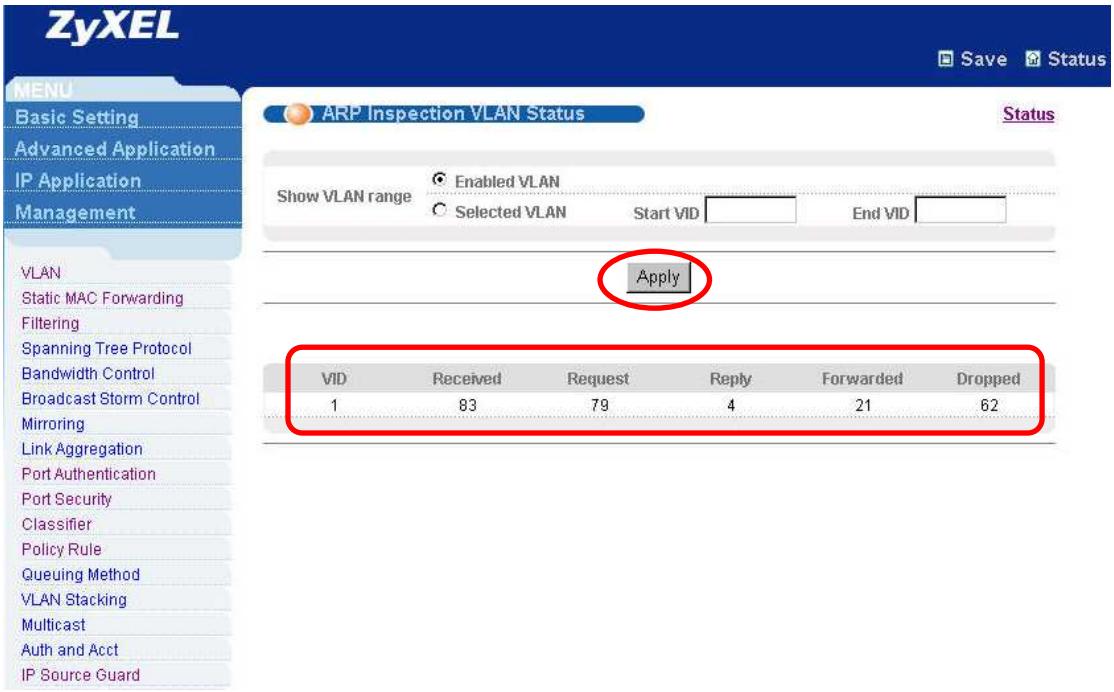


步驟 4：重新啟用電腦網路卡介面執行測試。

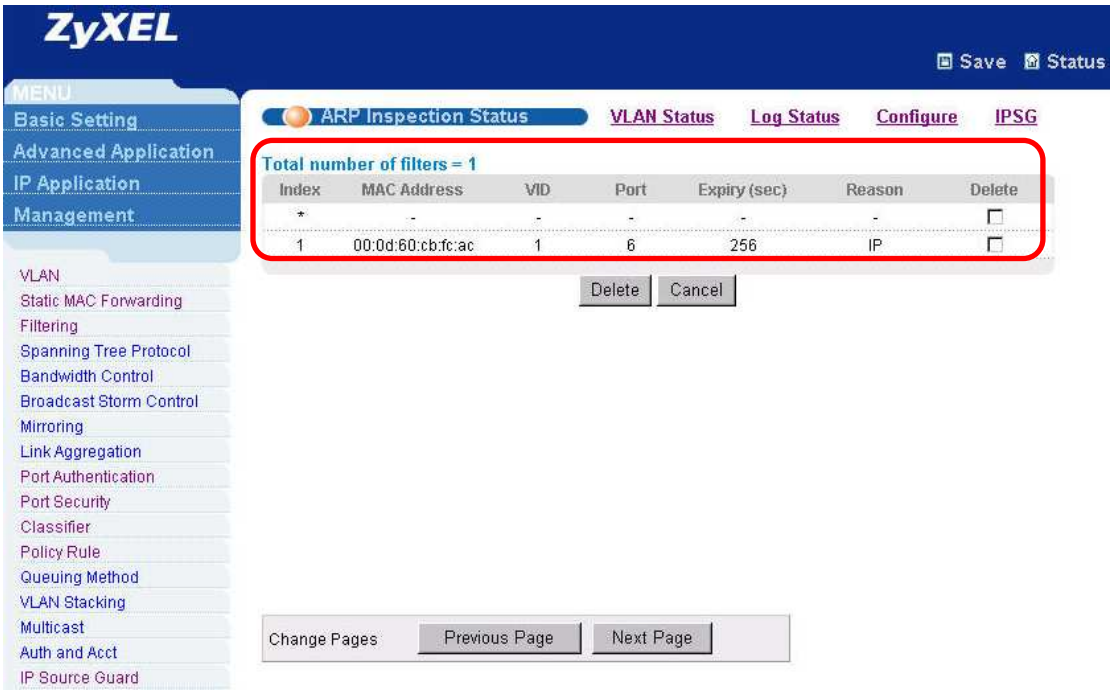
步驟 5：重新執行網路服務測試，例如：Ping HiNet DNS Server，此時會發現無法藉由 ARP Request 封包得知 Gateway MAC 位址，所以封包無法連接網際網路。

步驟 6：另外也可藉由網路封包擷取軟體驗證步驟五，確認為 NB 有發出 ARP Request 封包，但 Gateway 端卻無回應，原因為交換器將其 ARP 封包視為非法之 ARP 封包而丟棄，此部份可由步驟七來進行得知。

步驟 7：為查詢得知步驟五之 ARP 封包被交換器所偵測到並視為非法封包與之丟棄，請點選 **Advanced Application** > **IP Source Guard** > **ARP Inspection** > **VLAN Status**，此頁面請直接點選 **Apply** 進行有啟用 **ARP Inspection** 功能之 VLAN 的狀態觀看。在此可看到被丟棄的 ARP 封包數截至目前為止共 62 個。



步驟 8：切換回 **ARP Inspection 頁面**，在此頁面您可看到交換器將偵測到的非法 ARP 封包之來源 MAC 位址、VLAN 與拒絕之理由(即 Reason 欄位)一應俱全加以進行記錄。



請注意此頁面之 Expire 欄位，預設值為 300 秒，若任何非法日誌清單尚未過期之前，即使您將原本合法之網路設備變更回原始合法設定值後，也將無法正常運行。例如：以架構範例圖

為例，今交換器上已接上合法電腦可進行使用，但若使用者私帶其他電腦利用相同 Por 改串接該私有電腦，則該私有電腦一定無法進行使用，待使用者接回原本合法電腦，此時該合法電腦亦無法進行使用，原因為私有電腦非法之 ARP 封包已遭受交換器加以記錄，除非待該項日誌到期後，原本合法電腦才可再次進行任何網路服務使用。

End of the Document